Womersley Parish Council
Data Protection Policy

Introduction
Womersley Parish Council, as part of its day to day business, gathers and uses certain information about individuals. This can include employees, volunteers, parish officers business contacts and other third parties that the organisation has a relationship with. The Council recognises that that the correct and lawful treatment of this information will maintain confidence on the organisation and will provide for successful business operations.

Users of this information (or personal data) are obliged to comply with this policy when processing it.

This policy describes how this personal data must be collected, handled and stored to meet the Council's data protection standards – and to comply with the law.

Why this policy exists
This data protection policy ensures that the Council:

- Complies with data protection law and follows good practice and principles;
- Protects the rights of staff and any third party whose personal data is processed by the Council;
- Is open, clear and transparent about how it stores and processes individuals' data;
- Protects itself from the risks of a data breach.

Data Protection Law
Data protection rules, regulations and legislation regulate how organisations including the Council collect, handle and store personal information. The rules identified apply regardless of whether data is stored electronically, on paper or on other materials.

Personal data includes any data (including opinions and intentions) that can be used to identify a living individual. It also includes data which has been amended in such a way that it will only identify an individual when coupled with an identifying *key* (pseudonymised data). Should the Council handle such data it should consider what means are reasonably available to identify the individual that is the subject of the subject. Data which has been anonymised is not subject to data protection provided that the data subject cannot be identified by any means.

Personal data will be processed by the Council subject to the following principles:

- **Fair, lawful and transparent**:
  The Council is required to process data lawfully in accordance with the law as it applies to the Council at the time. The Council will advise the data subject what its data is to be used for (i.e. how it will be processed), the legal basis of the processing and will only process in this manner (i.e. it will not use the data for any purpose other than that which the data subject is aware). Any processing of personal data will be limited to that which is necessary to achieve the object of the collection of that data.
- **Accuracy**
  All data collected is to be accurate and kept up to date. Should data be out of date or not required then it should be deleted.

- **Be adequate, relevant and not excessive**
  Data held by the Council must be adequate and appropriate for the purpose for which it was collected. Where personal data is no longer required by the Council it should be deleted.

- **Be protected in appropriate ways**
  Data should only be handled in a manner which ensures the security of it. The Council should ensure that any personal data held by it cannot be unlawfully processed either by itself or a third party; that the data is secure and protected against accidental loss, destruction or damage.

Accountability
The Council is required to demonstrate how it complies with applicable data protection laws. As such, it will implement and maintain those policies and procedure necessary to achieve this.

People, Risks and Responsibilities
Policy Scope
This policy applies to:
- All offices of the Council
- All staff and volunteers of the Council
- All contractors, suppliers and other people working on behalf of the Council.

It applies to all data that the Council holds relating to identifiable individuals and includes:
- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Pseudonymised information
- IP addresses

Personal data must only be processed if there is a legal basis for it. The basis can be summarised as:

- Where consent has been acquired
- Where processing is necessary for compliance with a legal obligation
- For the performance of a contract or to take steps to enter into a contract
- To protect the vital interests of a data subject or another person.
- Where the processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the Council.

Certain information is regarded as forming part of a special category of data; this includes:
- Racial or ethnic origin;
- Political opinions or trade union membership;
- Religious, philosophical or other similar beliefs;
- Membership of trade unions;
- Physical or mental health or condition;
- Sexual life and orientation;
- Genetic or biometric data and
- Convictions, proceedings and criminal acts.

This information should only be handled (processed) where:
- Explicit consent has been provided by the subject of the data
- The personal data to be processed has already been made public by the subject
- Processing of this data is authorised or required by law
- The processing is necessary for the establishment of a legal claim

- Processing is necessary to protect the vital interests of the subject or of a natural person where the subject is physically or legally unable to give consent

Data Protection Risks
This policy helps to protect the Council from some very real data security risks, including:

- **Breaches of confidentiality** – for instance, information being disclosed unlawfully to a third party, lost, or inadequate security provisions being in place.
- **Failing to offer choice** - for instance, all individuals should be free to choose how the Council uses data relating to them.
- **Obtaining inadequate consent**. For instance where this is not freely given, or relates to another purpose
- **Reputational damage** – for instance, the Council could suffer damage to its goodwill if it becomes public knowledge that the organisation had lost personal data, or had been subject to a breach of security that could have been avoided.

Responsibilities
Everyone who works for or with the Council has some responsibility for ensuring data is collected, stored and handled appropriately. These individuals must:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.
- Understand fully the purposes for which the Council uses personal data.
- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the Council to meet its service needs or legal requirements.
- Ensure the information is destroyed securely when it is no longer required.
- Understand that breaches of this policy may result in disciplinary action, which may include dismissal

Each team that handles personal data must ensure that it is handled and processed inline with this policy and data protection principles.

The following people have key areas of responsibility:

- Councillors are ultimately responsible for ensuring that the Council meets its legal obligations.
- The Clerk is responsible for:
    - Keeping the Council updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data the Council holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The Clerk is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.

    - Evaluating any third-party services the company is considering using to store or process data.
- The Clerk is also responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing data protection queries from journalists or media outlets, such as newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who require it.
- Data should not be shared informally, and when access to confidential information is required, employees can request it from their line managers.
- The Council will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the Council or externally.
- Data should be regularly reviewed and updated. If it is found to be inaccurate then steps should be taken to remedy such inaccuracies. If no longer required, it should be deleted or securely destroyed.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Consent

Where the Council is required to obtain consent for the processing of personal data it shall do so in accordance with the law as it applies to the processing of data protection in force at the time, however shall do so in accordance with the following principles:

- Consent will be obtained with affirmative action on the part of the data subject.
- The data subject will freely provide such consent. Where possible, consent shall not become a precondition of a contract.
- The purpose of the requirement for the processing of data is clear and precise.
- Evidence of consent will be retained by the Council, which shall include, the date given, how it was provided, who provided it and who is aware of it. All documents which are used for obtaining consent shall be retained by the Council
- Consent will be reviewed to ensure that it is adequate and up to date.
- Names of third parties who are relying on the consent provided to the Council will be named in the consent.
- Data subjects will be told how consent to the processing of their data can be withdrawn by them. Any procedure for withdrawing consent shall be made as simple as possible by the Council.

Consent and children

Generally, children under the age of 16 are unable to provide consent to the processing of their data. If the Council is to process the personal data of a minor and requires consent to do so, it should obtain the consent of a parent or guardian of that child. Where consent is required and the child is aged 16 or over, consideration must be made to the purpose of the processing of the child's data,

and whether that child would understand the nature of the consent required. Where it is determined that a child is able to provide consent him/herself then the language of the consent must be adapted accordingly i.e. so that it can be understood by the intended reader.

Transfer of Data
A data subject's personal data may be transferred from the Council to another organisation, which will include (without limitation) another Council, or legal entity, such as the Church Commissioner of the Church of England, provided that there is a legal basis for the transfer, as below:

- The data subject has given his or her consent to the transfer – what does this entail? Would it include things such as employee references, for example?
- The transfer is necessary for the performance of a contract with the data subject
- The transfer s necessary for the implementation of pre-contractual measures taken in response to the data subject's request
- The transfer is necessary for the conclusion of performance of a contract concluded with a third party in the interests of the data subject
- The transfer is legally required on important public interest grounds
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary in order to protect the interests of the data subject

Data obtained from a third party
Where the Council obtains personal data from a third party (i.e. not from the data subject him/herself) the Council shall advise the data subject of the following:

- The identity of the person (which is likely to be an organisation) who controls the personal data, and (as appropriate) the details of its representative.
- The purpose for which the data is being processed (handled) and the legal basis for it
- The categories of personal data concerned

Data Storage
These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Clerk

When data is stored on paper, it should be kept in a secure place (such as a locked filing cabinet) where unauthorised people do not have access to it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people can see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.

- If data is stored on removable media (like a USB), these should be encrypted, password protected, and kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Personal data should only be retained for as long as is reasonably necessary. The data subject should be advised at the time of disclosure of its personal data the period that the data will be retained.

Data Use

Personal data is of no value to the Council unless it can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- Employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data should only be accessed by those individuals who require it.
- Where consent is used as the legal basis for the processing of data, the Council shall ensure that such consent is up-to-date and appropriate.
- Data must be encrypted before being transferred electronically. The IT provider can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area unless it can be demonstrated that adequate security is in place for the personal data transferred and/ or stored there.
- Copies of personal data should not be saved to devices other than those that are owned or controlled by the Council. Always access and update the central copy of any data.

Data Accuracy

The law requires the Council to take reasonable steps to ensure data is kept accurate and up-to-date.

The more important it is that the personal data is accurate, the greater the effort the Council should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up-to-date as possible:

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- The Council will make it easy for data subjects to update the information the Council holds about them. E.g. accessing the HR Toolkit.
- Data should be updated as inaccuracies are discovered. For instance, if an employee can no longer be reached on their stored telephone number, it should be removed from the database.

Data Subject Requests
All individuals who are the subject of personal data held by the Council are entitled to:

- Ask what information the company holds about them and why.
- The source of the persona data held by it.
- Details of any recipient third of any personal data processed by the Council.
- Ask how to gain access to it.
- Be informed how to keep it up-to-date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the Council requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by in writing email, addressed to the Clerk. The data subject making the request should be contacted in writing to advise who is dealing with their request and that it has been received.

Individuals will be charged £10 per access request. The Council will aim to provide the relevant data within 14 days but will otherwise advise the data subject of anticipated date on which the data will be available. The data controller should always verify the identity of anyone making a subject access request before handling over any information.

Data subjects have also the right to request the rectification of their data. In such circumstances the request shall be passed to the Clerk. Such requests must be acknowledged in writing and dealt with within 14 days. If the data subject's personal data has been disclosed to a third party, the Council shall advise that third party of its requirement to update the data held by it. The data subject will then be notified in writing of the action taken by the Council.

Disclosing Data for other reasons
In certain circumstances, the law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Requests may be considered where, the disclose is for the following purposes:

- The prevention or detection of a crime
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or duty
- By the order of a court or by a rule of law

Under these circumstances, the Council may disclose requested data. However, the Council is required to ensure the request is legitimate, and seek the assistance from the Council and from its legal advisers where necessary and appropriate.

Providing Information
The Council aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used;
- What data is being processed
- How long it will be retained
- How to exercise their rights.

The data subject must be informed of their right to complain should the Council have done something wrong, or be perceived to have. This right is to the supervisory authority in the United Kingdom, which is the Information Commissioners Office.

The Right to be Forgotten
The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data when there is no compelling reason for its continued processing however, the right to erasure does not provide an absolute 'right to be forgotten'.

Under specific circumstances, individuals do have a right to have their personal data erased and to prevent processing:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing processing.
- The personal data was unlawfully processed.
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Under the following reasons, a refusal to comply with a request is possible where personal data is processed:

- To exercise the right of freedom of expression and information; - we are slightly confused by what this actually means.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- The exercise of defence or legal claims.

If any personal data has been disclosed to a third party, it is vital to inform them about the erasure unless it is impossible or involves disproportionate effort to do so.